

ESTILS

Privacitat de sèrie als telèfons mòbils: prevenir i no curar

El 20% dels usuaris britànics que abandonen les xarxes socials ho fan pel neguit sobre les dades personals

NEREIDA CARRILLO
BARCELONA

Saps que els teus tuits poden reproduir la teva ruta si no has desactivat l'opció de geolocalització? ¿Ets conscient que algunes aplicacions del teu mòbil poden accedir als contactes del telèfon i esborrar-ne algun? Edward Snowden va obrir l'estiu passat els ulls als internautes en revelar l'espionatge massiu dels Estats Units. I la filtració de les fotos íntimes d'un centenar de famoses ara fa uns dies torna a subratllar la vulnerabilitat de la informació personal que confiï a internet. Els usuaris han deixat d'estar segurs que la seva privacitat està garantida i han començat a sospitar. Les empreses TIC reben més pressions per protegir les dades personals. I és en aquest context que pràctiques com la privacitat per disseny o la privacitat per defecte, abans desateses, ara troben altaveu; fins i tot s'inclouen en la nova normativa europea de protecció de dades. Reguladors i usuaris volen privacitat de sèrie.

L'enginyer de telecomunicacions Genís Margarit és un valador de la privacitat per disseny, la qual defineix com "anar al moll de l'os en lloc de posar la bena a la ferida". Aquesta pràctica reclama als desenvolupadors de productes tecnològics que pensin a protegir les dades personals ja en el moment del disseny del producte i

no a posteriori. Això evita possibles exposicions indesitjables de dades quan l'eina està en proves o ja en marxa. Margarit reconeix, però, que si bé la teoria és clara, només "els negocis més disciplinats" porten aquests principis a la pràctica.

Per l'enginyer, el cas de les fotos *hackejades* de les muses de Hollywood és un exemple més d'incompliment de la privacitat en el disseny. Apple ha negat cap error de seguretat a l'iCloud o a l'aplicació Find My iPhone (per localitzar i bloquejar un telèfon perdut) i ha culpant les víctimes de tenir contrasenyes massa fàcils. Però, per Margarit, l'empresa ha de prevenir situacions com aquestes –ho diuen els principis de la privacitat per disseny– i, per exemple, "obligar els usuaris a establir contrasenyes amb uns criteris mínims de dificultats".

Encriptar i controlar

Ann Cavoukian, durant 17 anys i fins fa poc comissionada per la informació i la privacitat d'Ontario, al Canadà, i impulsora dels principis de la privacitat per disseny, explica a l'ARA que garantir la privacitat en tot procés tecnològic resulta senzill.

Cal aplicar mesures com ara recollir només les dades que són necessàries, encriptar-les quan es recopilen i tenir un mapa del recorregut que fan dins d'una organització.

Des dels anys 90 aquesta experta intenta difondre arreu del món els 7 principis de la privacitat per disseny, que aquest estiu Margarit ha tradu-

ït al català. Entre d'altres, aquesta declaració preveu que la privacitat no sigui accessòria sinó inclosa en el disseny del producte, que la seguretat es persegueixi sempre i que s'informi amb claredat l'usuari. Per l'enginyer de telecomunicacions Jordi Bosch Garcia la realitat, però, és ben diferent: "Tothom és conscient que s'ha de tenir en compte la llei de protecció de dades. El problema és que la gent encara es pensa que gestionar les dades correctament és molt car i feixuc".

Privacitat per retenir clients

Bosch Garcia és el responsable a Espanya de Blue Bridge Technologies, una empresa letona de programari per al sector sanitari. La companyia ha guanyat aquest estiu l'accèssit del Premi de Protecció de Dades en el Disseny, que per segona edició ha convocat l'Autoritat Catalana de Protecció de Dades. L'aplicació guardonada, Inmedicas Secure Docshare, permet que els centres mèdics intercanviïn informació de manera segura. Bosch Garcia explica que avui dia s'envien documents mèdics per fax, per correu electrònic o per correu electrònic encriptat, però que cap d'aquestes trameses s'ajusta a la normativa. El sistema que proposen és una aplicació web que simula un fax però és més segura. Bosch Garcia explica que per entrar-hi cal identificació; després el metge diposita el document que vol enviar, com ara els resultats d'una anàlisi de sang, en una mena de caixa forta digital a la qual només la persona autoritzada té accés. Cal que la identitat del destinatari es verifiqui presencialment.

Cavoukian, ara directora de l'Institut de la Privacitat i el Big Data de la Universitat de Ryerson, considera que la protecció de les dades és estratègica: "El que els dic a les empreses és que, a llarg termini, si incorporen la privacitat per defecte en la



ESCLETXES DE SEGURETAT
01 i 02. Les actrius Jennifer Lawrence i Kate Upton són algunes de les famoses a qui van robar fotografies íntimes. GETTY IMAGES



Privacitat
S'envien documents mèdics per correu sense ajustar-se a la normativa

seva configuració creixerà la confiança i la lleialtat dels seus usuaris". Fins ara, però, moltes empreses TIC han seguit la direcció contrària: "En sis anys Facebook ha canviat set o vuit cops la seva política de privacitat. I cada vegada l'ha canviat per reduir més la intimitat dels seus usuaris. Jo no tinc Facebook i em vaig donar de baixa de WhatsApp quan el va comprar Facebook perquè no me'n refio", explica Margarit, i no és l'únic desconfiat.

Segons un estudi de l'empresa britànica d'anàlisi demoscòpica YouGov, el 20% dels usuaris britànics que abandonen les xarxes socials ho fan empesos per la preocupació sobre la seva privacitat. A més de la privacitat en les xarxes socials, la filtració de fotos de famoses ha sigut un crit d'alerta sobre la seguretat del núvol. Margarit recomana tenir dobles factors d'autenticació –com ara l'autenticació en dos pa-



sos de Gmail-, bloquejar els dispositius que no siguin de confiança o encriptar les comunicacions amb eines com ara WhisperSystems.

Dades massives, però bones

El neguit per les dades personals comença a erosionar la confiança en les empreses TIC. Els reguladors volen que s'hi imposi la privacitat per defecte, és a dir, que la privacitat estigui garantida sense que l'usuari hagi d'anar a les configuracions i desactivar alguns permisos. És a dir, que no s'hagi d'anar desactivant en cada xarxa social o aplicació de mòbil l'opció de geolocalització, l'opció que tot-hom i no només els seus amics vegin els continguts, etc. "Gràcies a la literatura acadèmica sabem que en un 80% de casos el que estigui configurat per defecte és el que prevaldrà. I vull que això sigui la privacitat", explica a l'ARA Cavoukian. Aquesta lluitadora per la privacitat explica



Seguretat
El 80% de
les persones
no retoquen
les condicions
que els vénen
per defecte

que és una fal·làcia creure que hem de triar entre privacitat i seguretat pública –una idea estesa pel govern de Bush després dels atemptats de l'11-S– o entre privacitat i serveis gratuïts. "Podem tenir totes dues coses. Triar és més fàcil però cal ser més creatiu per tenir-ho tot", diu.

La protecció de la privacitat també s'ha d'estendre al *big data*. Cavoukian assegura que, a banda de massives, les dades han de ser "bones". "Hem d'insistir que la privacitat estigui incorporada en el procés. Una de les maneres és incloure protocols d'anonimització de dades molt forts i combinar-los amb entorns de risc de reidentificació febles, que estiguin per sota de l'1%". L'experta insisteix que, malgrat l'"expectativa natural de privacitat" que té l'usuari, cal que sigui més responsable. No pot donar res per garantit, no en l'era post-Snowden. —